Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (809-822)

Criminological Characterization of Internet Fraud: Experience of the Republic of Kazakhstan

Khamit Edil[1], Mukhamadieva Gulnar[2], Togaibaeva Sholpan*[3],
Mashabayev Amanbek[4], Salykova Aliya[5], &
Karakushev Salimgerey[6]

Abstract

This article examines statistical data on internet fraud in the Republic of Kazakhstan from 2019 to 2023. It delves into the key demographic and social characteristics of both perpetrators and victims, identifying trends in the dynamics of internet fraud. The analysis uses statistical data to explore the age, gender, and occupational characteristics of those involved, with a focus on the most active age groups and the notably high proportion of unemployed individuals among the criminals. The authors highlight the need for improvements in law enforcement practices to better prevent internet fraud, which currently does not match the scale and dynamics of these crimes. New forms of internet fraud, such as online credit fraud and phishing—prevalent types in Kazakhstan—are discussed. The novelty of this work lies in the proposal of specific preventative measures derived from an analysis of international practices and law enforcement experiences in Kazakhstan.

Keywords: internet fraud; crime prevention, cybersecurity, law enforcement, statistics, criminal identity, criminological characterization

Introduction

At this stage of information technology development, the Internet has become an integral part of daily life and a crucial component of our economic and social systems. As the number of web users increases, so too does the occurrence of crimes

[1] Master of Law, Doctoral student of the Faculty of Postgraduate Education, Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Barimbek Beisenov, Karaganda, Republic of Kazakhstan. Email: neofartflirt@mail.ru
[2] Candidate of Legal Sciences, Head of the Department of Criminal Law and Criminology, Karaganda Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan named after Barimbek Beisenov, Karaganda, Republic of Kazakhstan. Email: gmuhamadieva@mail.ru
[3] Candidate of Legal Sciences, Professor of the Department of "Jurisprudence", Myrzakhmetov Kokshetau University, Kokshetau, Republic of Kazakhstan. *He is also the corresponding author. Email: togaibaeva@mail.ru
[4] Candidate of Legal Sciences, Associate Professor, Professor of the Department of Criminal Law, Process and Criminology, Buketov Karagandy University, Karaganda, Republic of Kazakhstan. Email: mashabaev.a@mail.ru
[5] Candidate of Law, Senior Lecturer, Department of Criminal Law, Process and Criminology, Buketov Karagandy University, Karaganda, Republic of Kazakhstan. Email: aliya-salykova@mail.ru
[6] Candidate of Law, Head of the Department of Jurisprudence, Myrzakhmetov Kokshetau University, Republic of Kazakhstan. Email: science_future@mail.ru

commit in cyberspace, particularly internet fraud. This type of crime typically involves unauthorized access to data, deception, or abuse of user trust, resulting in financial losses (AlFreihat et al., 2023). In recent years, Kazakhstan has seen a significant rise in internet fraud cases, spurred by the expansion of digitalization and e-commerce.

Internet fraud is not just a technological issue but a social problem as well. Unlike traditional fraud, where criminals interact directly with their victims, internet fraud features anonymity and latency, significantly complicating crime investigations. This often results in many criminals going unpunished, while the number of affected individuals and organizations continues to rise (Zholzhaksynov, 2022).

Studying internet fraud in Kazakhstan is essential for several reasons. The high latency of these crimes makes them difficult to detect and resolve, while an inadequate legal framework complicates the proper classification and prosecution of cyber fraud. Furthermore, the increase in internet fraud threatens the national economy and erodes public trust in financial and governmental institutions. This research offers a comprehensive criminological analysis specific to Kazakhstan, incorporating local legal, social, and technological dimensions. It updates the criminological profile of internet fraud, highlighting both general trends and distinctive local features.

Literature Review

Research on internet fraud is crucial both within Kazakhstan and globally. In Kazakhstan, scholars like Togaibaeva et al. (2016) and Lakbayev et al. (2020) focus on general aspects of information security and law enforcement practices. Others, such as Zholzhaksynov Zh. and Darmenov A. (2022), explore the dynamics of crimes linked to informatization, noting the investigative challenges and high latency in Kazakhstan. Researchers like Almazkyzy K. (2018) and Batotsyrenov B. (2021) consider cybercrime a national security threat and advocate for stricter legal control over information resources.

Internationally, experts like Shumikhin V. and Tretiak M. (2014) in Russia, and Potapova A. (2020) contribute to understanding the legal and criminological aspects of internet fraud. Anderson R. and Moore T. (2019) emphasize the transnational nature of internet fraud, advocating for international legal cooperation. In the U.S., scholars such as Levi (2021) highlight the exploitation of cyberspace for financial crimes.

Despite numerous existing studies, this article offers significant value by focusing on the criminological characteristics of internet fraud within Kazakhstan's unique national context. It addresses the challenges of crime classification and the need for more refined legal norms. As digital spaces and financial transactions expand, there is a critical need for enhanced preventive and law enforcement

measures. This study aims to provide a deeper criminological analysis, underscore unique local features, and propose legislative enhancements to effectively combat internet fraud.

Research Questions

This study will answer the following main question:

- What are the unique criminological characteristics of internet fraud in the Republic of Kazakhstan?
- What motivates the commission of internet fraud in Kazakhstan?
- What personality traits of criminals committing internet fraud can be identified through statistical analysis?
- What characteristics of internet fraud victims can be identified through statistical analysis?
- What preventive measures and strategies are effective in combating internet fraud in an increasingly digitalized context?

Research Objectives

This study aims to achieve the following primary objectives:

- Analyze the criminological characteristics of internet fraud in the Republic of Kazakhstan.
- compile criminological profiles of both internet fraud perpetrators and victims.
- develop proposals for preventing internet fraud, based on the findings of this study.

Research methods

This study employed both qualitative and quantitative methods to analyze internet fraud in Kazakhstan, utilizing data from the Legal Statistics Portal of the General Prosecutor's Office. It included statistical analysis and content analysis of Kazakhstani criminal legislation to assess the extent of internet fraud and the effectiveness of countermeasures. The criminological analysis identified the socio-demographic characteristics of criminals, shedding light on the connection between their backgrounds and crime-committing methods. Furthermore, the study evaluated law enforcement practices by reviewing criminal cases, which highlighted issues such as insufficient training and challenges related to the anonymity of cybercrime. A comparative legal analysis with international practices suggested ways to enhance Kazakhstan’s strategies for combating cybercrime.

Results and discussion

The analysis of specialized literature by Kazakhstan's (Zhatkanbayeva, 2009; Almazkyzy, 2018) and international (Kvasnikova et al., 2019; Komarov, 2011) researchers has led to the conclusion that the main causes of internet fraud are multifaceted. Firstly, the psychological vulnerability of individuals plays a significant role. Fraudsters often possess advanced manipulation skills, enabling them to easily gain the trust of potential victims. These victims are generally gullible and exhibit low vigilance, often seeking quick gains with minimal effort (Batotsyrenov et al., 2021). Secondly, the organization of software security is weak. Existing security measures frequently fail to keep pace with the continually advancing fraudulent methods.

The third factor concerns the inefficiency of law enforcement agencies. Monitoring of internet spaces and messaging services is not consistently effective, compounded by a shortage of specialists with the necessary information technology skills.

Research has shown that internet fraud in the Republic of Kazakhstan is on the rise, a trend supported by statistical data. The resolution rate of criminal cases related to internet fraud is disappointingly low. The study also indicates that the increase in registered internet fraud crimes correlates with the growth of the digital infrastructure and the rising number of internet users. Additionally, the high latency of these crimes hinders their detection and results in substantial social and economic losses (Zholzhaksynov, 2022; Norris et al., 2019).

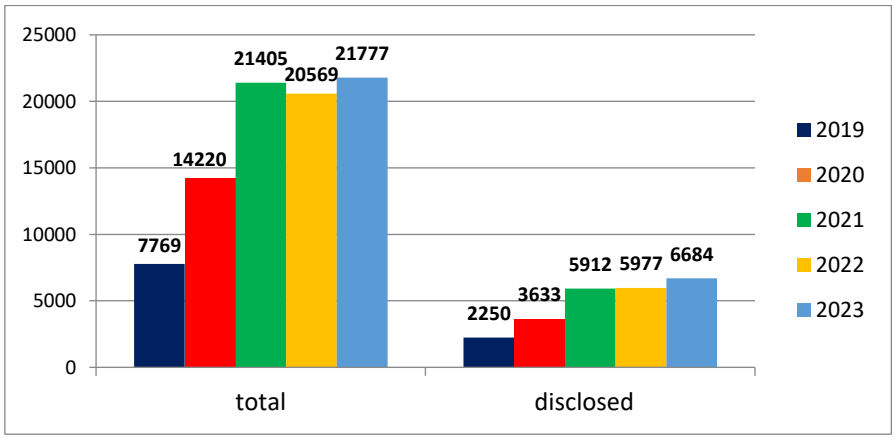

Figure 1. Number of reported Internet frauds and unsolved criminal cases of this type

Our study of the identity of internet fraudsters, based on statistical data, reveals the following results:

1. An analysis of the age composition of internet fraudsters from 2019 to 2023 indicates a clear trend toward an increase in the number of offenses committed by individuals aged 18 to 49 years. Notably, the most significant concentration of offenders is within the 21-29 year age group, which consistently

ranks highest in the number of offenses throughout the period reviewed. From 2020 onwards, there has been a noted increase in offenses among those aged 30-39 years, suggesting an expansion in the age range of individuals involved in internet fraud. Interestingly, there is a decrease in activity among the 14-15 years and 60+ years age groups, which we believe is due to a lack of necessary technical skills or reduced motivation to engage in illegal activities (Table 1).

Table 1. Age composition of internet scammers.

years	14-15	16-17	18-20	21-29	30-39	40-49	50-59	60 and higher
2023	0	133	620	2490	2259	800	283	60
2022	1	54	289	1473	1358	486	174	44
2021	0	78	363	2323	2045	768	327	183
2020	0	90	404	2700	2300	950	384	159
2019	0	134	520	3022	2619	1066	576	178

2. An analysis of data on the citizenship and gender of internet fraud perpetrators from 2019 to 2023 reveals several key patterns (Table 2). The vast majority of internet fraudsters are citizens of the Republic of Kazakhstan, underscoring the domestic nature of these crimes. The proportion of offenders from CIS countries and other foreign nations remains exceedingly small, never exceeding 2% of the total number of offenders. This may suggest significant barriers to entry for foreign groups or more effective measures for controlling cross-border crime in Kazakhstan.

Regarding gender, there is a consistent trend: the overwhelming majority of offenders are men, accounting for about 70% each year. Although there has been a slight increase in the number of women involved in internet fraud—from 1,812 in 2022 to 1,946 in 2023—their representation remains considerably lower compared to men. This disparity highlights gender-specific differences in motivation and access to technology, as well as variations in criminal behavior between men and women, as noted by international researchers (Goulette, 2020; Wibowo, 2024).

Table 2. General information on the nationality and gender of Internet scammers

years	Total persons	RK citizen	CIS citizen	Foreign citizens	women	men
2023	6645	6409	103	7	1946	4699
2022	6071	5723	91	15	1812	4259
2021	6087	5743	113	18	1915	4172
2020	6987	6648	144	7	2184	4803
2019	8115	7704	149	8	2509	5606

3. From 2019 to 2023, an analysis of the occupations of internet fraudsters reveals significant insights into the social structure of crime perpetrators. During this period, a considerable majority of these criminals were unemployed, indicating a correlation between economic hardship and the propensity for unlawful activity. In 2023, unemployed individuals accounted for 83.4% of the offenders, maintaining a consistent trend from 2019, when the figure was 83.5%. This data strongly suggests a link between unemployment and participation in internet fraud.

The involvement of students, especially those from higher education institutions, is also noteworthy. In 2023, students constituted 1.36% of fraudsters, with university students making up 58.9% of this demographic, highlighting significant issues within educational environments related to digital access and legal literacy.

The data also shows limited criminal participation among civil servants and private entrepreneurs, likely due to stricter oversight and fewer opportunities for engaging in internet fraud. In 2023, only 1.46% of fraudsters were government employees, a decrease from 3.13% in 2019, reflecting increased monitoring. The percentage of private entrepreneurs involved in fraud also decreased from 1.77% in 2019 to 1.25% in 2023, further emphasizing the impact of regulatory measures (Table 3).

Table 3. Occupation of Internet fraudsters

	Workers	Civil servants	Private entrepreneurs	Pupils				Unemployed	Education		military personnel	of which				Other persons
				total	Schools, gymnasiums	colleges	universities		Higher	Secondary specialized secondary		officers	contract servicemen	ordinary employee	Other	
2023	235	97	83	90	10	53	27	5539	1768	4754	21	5	18	6	10	601
2022	193	165	96	59	5	39	15	5035	1617	4349	12	5	11	3	4	523
2021	154	150	122	54	11	33	10	4957	1602	4389	13	7	9	3	3	650

2020	216	223	107	61	10	38	13	5824	1630	5245	25	7	25	3	15	556
2019	213	254	144	106	16	57	33	6776	1882	6058	26	9	25	5	12	622

A comparative analysis with international practices, particularly studies from the United States and the United Kingdom, has shown that cybercriminals employ similar deceptive techniques such as phishing, creating fake websites, and manipulating personal information (Hawdon, 2021; Shang et al., 2023). These techniques are prevalent across both the dark and open web, making them accessible even to criminals with relatively low technical skills (Hawdon, 2021). Crucially, internet frauds often occur under insufficient law enforcement surveillance, allowing fraudsters to exploit platforms like social media and email to achieve their objectives (Norris et al., 2019).

Furthermore, the analysis of data from a sociological survey reveals that the diversity of methods used to commit internet fraud presents challenges in classifying these crimes accurately for investigators. According to the survey, 68% of respondents, who are current employees of investigative units in the Republic of Kazakhstan, reported difficulties in determining the correct classification of cyber thefts (Fig. 2).

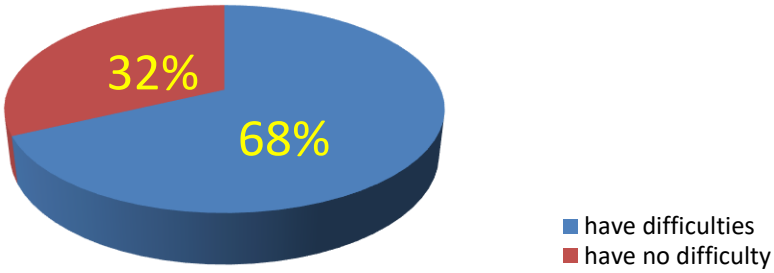

Figure 2. Percentage of respondents' answers to the question about difficulties in determining the qualification of Internet frauds

A criminological analysis of internet fraud in Kazakhstan has identified several key factors that influence the development of this crime type. One notable feature is the high degree of anonymity the internet offers to criminals, complicating their identification and the subsequent investigation of criminal cases. Initial information plays a crucial role in the registration of a crime, and as various international studies have highlighted, criminals employ methods like fake accounts, virtual private networks (VPNs), and data encryption technologies to conceal their identities (Norris et al., 2019; Shang et al., 2023).

The causes of crime refer to the underlying factors and phenomena that precipitate the commission of criminal offenses (Kuznetsova, 2004).

An analysis of statistical data over the last five years indicates that internet fraud represents a significant proportion of cybercrimes (Table 4). Compared to traditional frauds, internet fraud occupies a leading position (Table 5), underscoring the need for a more detailed investigation into the causes of these illegal acts. This will aid in developing effective preventive measures to reduce their prevalence.

Table 4. Information on registered facts of Internet fraud and criminal offenses under Chapter 7 of the Criminal Code of the Republic of Kazakhstan for 2019-2023

Type of criminal offense	Total registered				
	2019	**2020**	**2021**	**2022**	**2023**
Internet - fraud (paragraph 4, part 2, article 190 of the Criminal Code of the Republic of Kazakhstan)	7769	14220	21405	20569	21777
Total number of offenses under Chapter 7 of the Criminal Code of the Republic of Kazakhstan	108	110	74	85	78

Table 5. Information on reported fraud perpetration for 2019-2023

	2023	2022	2021	2020	2019
Types of fraud in Kazakhstan	TOTAL				
by borrowing money	21	94	121	41	66
on credit	29	551	89	9	6
payment card fraud	170	237	353	468	66
Internet fraud	**21777**	**20569**	**21405**	**14220**	**7769**
in the field of land law relations	3	1			
real estate	0	4	1		

One key aspect emphasized in criminology is the motive of criminals. Internet fraudsters are often driven by self-interest and a sense of impunity. This behavior is supported by "risk denial" theories, which propose that criminals minimize the perceived risk of being caught by comparing their actions to more severe crimes and justifying their own behavior due to the relatively "soft" nature of internet crimes (Offei et al., 2019). In Kazakhstan, this trend is particularly noticeable against a backdrop of sometimes ineffective law enforcement practices and insufficient technical equipment, which gives fraudsters a high degree of confidence in their impunity (Zholzhaksynov, 2022).

Our research indicates that the most prevalent types of internet fraud in Kazakhstan involve schemes that use fake websites to apply for online loans and phishing attacks. These methods enable criminals to extract personal data from victims for later illegal use (Khamit, 2023). Additionally, the illegal issuance of online loans is notably frequent, reflecting the popularity of lending among Kazakhstan's residents. The volume of retail loans issued in 2021 surged by 83.6% from the previous year, reaching 8.9 trillion tenge. In 2023, there was a further 73% increase from the previous year, with 208.4 thousand loans issued (Andreeva, 2024). This growth is fueled by the rapid development of network technologies and the internet amidst global political and other processes (Vestov, 2020). Often, victims do not realize they are being defrauded when using falsified websites or applications from credit organizations. It is also noteworthy that many fraudsters are skilled psychologists who easily gain the trust of potential victims (Adambekova, 2018).

Data analysis on the victims of internet fraud from 2019 to 2023 shows significant shifts in the demographic composition of the victims, as well as the extent of offenses against different groups. In 2023, there were 43,918 offenses against individuals, marking a 2.58% increase from 2022. The number of female victims rose from 25,342 in 2022 to 26,813 in 2023. The number of minors affected by internet crimes decreased dramatically to 31 in 2023 from 120 in 2022, indicating an increased legal vulnerability for this demographic.

The number of disabled persons among the victims has significantly decreased: only one person was affected in 2023, compared to 11 disabled persons in 2022, marking a 90.9% reduction. Similarly, the number of pensioners affected by internet fraud decreased from 1,372 in 2022 to 529 in 2023, a 61.4% decrease. These figures indicate improved protection for vulnerable groups and the effectiveness of preventive measures.

Regarding the age composition of victims, in 2023, the most affected age group was those aged 30-39 years, with 13,036 persons affected, representing 29.7% of all victims. In 2022, this group was also the largest, with 12,832 persons, accounting for 30% of the victims. Those over 60 years old were the least victimized, but their proportion has gradually increased from 2,135 in 2019 to 6,420 in 2023, suggesting an increase in internet crimes against older citizens.

When examining citizenship, the majority of victims in 2023 were citizens of the Republic of Kazakhstan, totaling 6,908 people (15.7%). The proportion of foreign citizens and stateless persons remains low, with their numbers varying between 23 and 107 people throughout the analyzed period (Table 6).

Table 6. victim information

Total	victims

	including					in relation to and citizens				against persons by age					
	women	underage	invalids	pensioners	convicts	RK citizens	CIS citizens	Foreign citizens	Stateless persons	18-20 age	21-29 age	30-39 age	40-49 age	50-59 age	60 age and hogher
2023															
43918	26813	31	1	529	3	6908	79	107	23	2917	8905	13036	10104	6891	6420
	2022														
42811	25342	120	11	1372	8	43158	462	87	63	2789	9077	12832	9528	6212	4113
	2021														
40100	23337	96	9	1286	9	40023	579	71	44	2376	9685	12488	8420	4906	3274
2020															
232495	18458	76	9	761	9	32182	502	69	39	1522	8570	10438	6708	3675	2076
2019															
30570	16487	102	10	720	11	30959	502	71	22	1657	8595	9529	6068	3588	2135

Generalized data encompassing all types of fraud were utilized to develop a profile of the victims, as official statistics do not specifically categorize internet fraud. The socio-demographic characteristics of internet fraud victims likely resemble those of traditional fraud victims, permitting the use of aggregated data for preliminary analysis. Research indicates that a significant proportion of internet fraud victims possess limited digital security knowledge, heightening their vulnerability to phishing and fraud. Additionally, psychological factors such as the perpetrator's sense of impunity and the victims' diminished risk awareness play a substantial role in the prevalence of internet fraud, as highlighted in various international studies (Shang et al., 2023; Offei et al., 2019).

Conclusion

A comprehensive analysis of internet fraud in Kazakhstan from 2019 to 2023 reveals a steady increase in crimes, coinciding with rapid digitalization and the expanded use of online financial services. This upsurge poses significant threats to individual security and economic stability. Predominantly, male citizens aged 18-49, who are often unemployed or students, are involved in these crimes, suggesting a correlation between economic challenges and criminal behavior. Vulnerable groups, particularly those aged 30-39 and over 60, are most affected, underscoring the need for enhanced digital literacy and cybersecurity measures. The anonymity afforded by the internet complicates the detection and prosecution of these crimes, resulting in low case resolution rates. Furthermore, modern phishing and social engineering techniques are prevalent, exploiting vulnerabilities in software and digital platforms. As the digital infrastructure continues to grow, it is crucial for Kazakhstan's legal framework to evolve in order to effectively counter these emerging cyber frauds.

Recommendations

This study recommends that:

1. As a significant portion of offenders falls within the 18-49 age group, particularly those aged 21-29 and 30-39, prevention efforts should prioritize educational campaigns aimed at this demographic. Implementing digital literacy programs in schools, universities, and workplaces to raise awareness of the consequences of internet fraud will help reduce involvement in such activities.
2. Given the high percentage of unemployed individuals involved in internet fraud, measures should be taken to alleviate economic insecurity. Offering employment opportunities and social support programs for at-risk groups can diminish the likelihood of individuals engaging in internet fraud for financial gain.
3. Considering that many offenders are students, particularly from higher education institutions, enhancing cybersecurity within educational environments is crucial. Universities and colleges should integrate cybersecurity awareness into their curricula, educating students on the ethical use of technology and the legal repercussions of participating in internet fraud.
4. The data indicates an increase in the number of elderly victims, signaling the need for more focused cybersecurity education for this group. Government initiatives should be launched to boost digital literacy and awareness among older adults, emphasizing the recognition of fraudulent schemes such as phishing and fake websites.

References

Adambekova, A. (2018). New requirements for bank risk management and organization of banking supervision. *Central Asian Economic Review*, 5-6, 130-145.

AlFreihat M.S., Al Wahshat Z.M., Balas H.A.M. & Abueid A. (2023). Fraud as a Reason to Book a Documentary Credit. *Pakistan Journal of Criminology*, 4 (15), 213-222;

Almazkyzy, K. (2018). Cybercrime as a new criminal threat to the security of the Republic of Kazakhstan. *Bulletin of the Kazakh National University. Legal Series*, 4 (88), 142-151;

Anderson R. & Moore T. (2019). The Economics of Information Security. *Science*, 2, 610-620;

Andreeva, D. (2024). Mortgage, car loans, bankruptcy of individuals: the results of the credit market of Kazakhstan for 2023. *Kazakhstan Forbes*. https://forbes.kz/articles/ipoteka_avtokreditovanie_i_bankrotstvo_fizlits_itogi_kreditnogo_ryinka_rk_za_2023_god_1

Batotsyrenov, B., Darmayev, A. & Kupriyanov, D. (2021). Digital fraud. *Criminological Readings: Proceedings of the XVI All-Russian Scientific and Practical Conference dedicated to the 300th anniversary of the Prosecutor's Office of Russia*, Ulan-Ude, 167-175.

Darmenov, A. & Zholzhaksynov, Zh. (2022). Features of the personality of the victim of cybercrime in the Republic of Kazakhstan. *"Khabarshy - Vestnik" of Karaganda Academy of MIA RK named after B. Beisenov*, 3 (77), 42-43;

Goulette, N. (2020). What are the gender differences in risk and needs of males and females sentenced for white-collar crimes? *Criminal Justice Studies*, 33(1), 31–45.

Hawdon, J. (2021). Cybercrime: Victimization, Perpetration, and Techniques. *American Journal of Criminal Justice*, 46, 837–842;

Khamit, E. (2023). Features of qualification of Internet thefts committed by means of "phishing". *Bulletin of the Academy of Law Enforcement Agencies*, 3 (29), 67-75.

Komarov, A. (2011) Criminological aspects of fraud in the global network; dissertation of candidate of legal sciences. Saratov State Law Academy publishing, Saratov.

Kuznetsova, N. & Luneeva, V. (2004). Criminology: Textbook. Walters Kluwer Publishing House, Moscow.

Kvasnikova, T., Levsha, N. & Korobeinikov, I. (2019). Criminological characteristics of fraud in the Internet. *Diary of Science*, 12 (36), 43-50.

Lakbayev, K., Rysmagambetova, G., Umetov, A., Sysoyev, A. (2020). The crimes in the field of high technology: Concept, problems and methods of

counteraction in Kazakhstan. *International Journal of Electronic Security and Digital Forensics*, 12(4), 386–396

Levi M. (2021). Cybercrime and Financial Crimes: A Review of the Literature. *Journal of Financial Crime,* 3, 98-112;

Norris, G., Brookes, A. & Dowell, D. (2019). The Psychology of Internet Fraud Victimisation: a Systematic Review. *Journal of Police and Criminal Psychology,* 34, 231–245

Offei, M., Kofi, F., Baidoo, A., Ayaburi, E. & Asamoah, D. (2019). Understanding Internet Fraud: Denial of Risk Theory Perspective. *ICT Unbounded, Social Impact of Bright ICT Adoption,* 558, 415-424.

Potapova, A. (2020). Fraud in the Internet: criminological characterization and problems of qualification. *Student*, 6, 52-57;

Sadvakasova, A. & Khanov, T. (2019). On the new system of recording and registration of complaints, statements and other information on criminal offenses. *Russian journal of criminology,* 13(2), 340–353.

Shang, Y., Wang, K., Tian, Y., Zhou, Y., Ma, B. & Liu S. (2023). Theoretical basis and occurrence of internet fraud victimisation: Based on two systems in decision-making and reasoning. *Frontiers in Psychology, 14.* https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2023.1087463/full

Shumikhin, V. (2014). The seventh form of theft of another's property. *Vestnik of Perm University. Juridical Sciences*, 2, 229-233;

Togaibaeva, S, Togaibaev, I., Khanov, A., Sikhimbayev, R. & Rustemova, G.R. (2016). Criminal liability for illegal actions concerning insider information in the republic of Kazakhstan. *International Journal of Environmental and Science Education*, 11(17), 10197–10209;

Tretiak, M. (2014). Rules of qualification of computer fraud and crimes under Ch. 28 of the Criminal Code of the Russian Federation. *Criminal Law*, 4, 69-74;

Vestov, F. (2020). Criminal policy on the use of digital technology capabilities in countering fraud. *Fundamentals of Economics, Management and Law,* 6 (25), 53-57.

Wibowo, D. (2024). Women behind the veil: Power and lifestyle in workplace fraud. *Journal of Infrastructure, Policy and Development*, 8 (8), 5906.

Zhatkanbaeva, A. (2009). Functional components of information security. *Collection of materials from the conference "Contribution of young researchers in industrial-innovative development of Kazakhstan".* https://articlekz.com/article/6782;

Zholzhaksynov, Zh. (2022). Determinants of committing Internet fraud in the Republic of Kazakhstan. *Modern directions of improvement of the legal system and legal education of the Republic of Kazakhstan.* Karaganda University named after E.A. Buketov. E.A. Buketov publishing, 416-420.